

Orion Threat Alert: Flight of the BumbleBee

 cynet.com/orion-threat-alert-flight-of-the-bumblebee/

April 14, 2022

Orion Threat Alert



By: Max Malyutin – Orion Threat Research Team Leader

Orion, Cynet’s Threat Research and Intelligence team, spotted a new malware campaign in the wild: BumbleBee.

Wondering what’s going on? Let us fill you in.

We noticed a new trend in Initial Access Brokers’ (IAB) tactics to gain access to their victims’ machines. Initial Access Brokers refers to a cybercrime group that specializes in gaining initial access to organizations for the sole purpose of offering it to other threat actor groups. The trend started earlier this year and our team recently spotted their new BumbleBee campaign.

Usually, we observe malicious spam (MalSpam) campaigns that deliver malicious documents (MalDoc) to lure the victims to interact with the MalDoc and execute the malicious macro code by clicking “Enable Content.” That in turn downloads and executes the malicious payload, for example, [the notorious Emotet campaigns](#).

We expected these groups to change the initial access methods. We believe there is a direct relation to the changes Microsoft applied recently to the default policy in their Office products: “[Macros from the internet will be blocked by default in Office](#)” and “[Excel 4.0 \(XLM\)](#)”

macros are disabled by default.” These changes impact IABs because they have been abusing Office documents with malicious macros for years.

It appears that they’ve come up with a plan B.

In this post, we will cover what this campaign is, and how the IAB distributes the BumbleBee malware and its TTPs. We will also explain each TTP according to the MITRE ATT&CK model, and its purpose.

A new campaign in the wild: BumbleBee

From our initial analysis, BumbleBee is a custom new loader that is used by different IAB groups. This malware was observed injecting Cobalt Strike shellcodes in memory and using several tactics, techniques, and procedures (TTPs) in order to compromise the victim’s environment.

As part of the campaign, the threat actors abuse spoofed companies’ identities (like fake employee email addresses, fake websites, etc.) and use legitimate public storage services to deliver the malicious ISO image file. The ISO image file is responsible for luring the victim to execute the BumbleBee malware.

We’ve seen Living Off the Land Binaries (LOLBins) execution with rundll32, which allows threat actors to avoid defenses. BumbleBee also creates a scheduled task on the compromised host for persistence and executes a Visual Basic script via the scheduled task. The IAB relies on the user (victim) execution to execute the BumbleBee payload by luring the victim to mount an ISO image file and click on a Windows shortcut (LNK) file.

The malware name, BumbleBee, was chosen because of its unique user agent, “bumblebee,” that was used as part of the communication with the command and control server (C2).

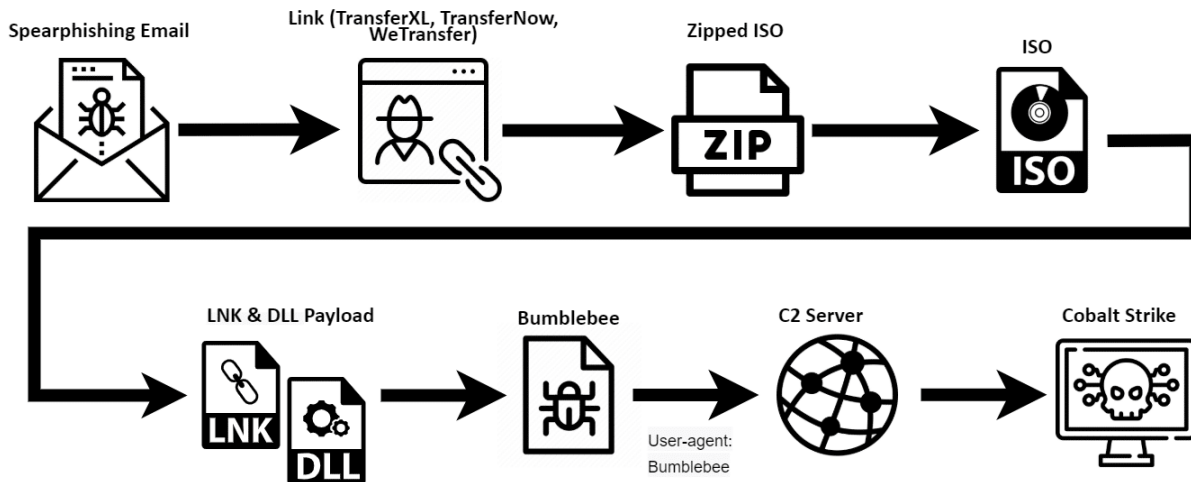
Threat Analysis Group (TAG) shared observations on the financially motivated threat actor, EXOTIC LILY, that use the BumbleBee malware. In addition, TAG mentioned an interesting point of collaboration between EXOTIC LILY and the WIZARD SPIDER threat group.

Orion’s observations

This type of attack is new, and the cybersecurity community is still gathering data to glean more insights on the nature of this attack and its targets.

Orion found a high number of targeted companies based in the US with the following distribution method that delivers the BumbleBee malware: Spear phishing email > URL Link (TransferXL, TransferNow, WeTransfer) > Zipped ISO > ISO (contains the LNK file and the BumbleBee payload).

You can see the execution flow in the image below.



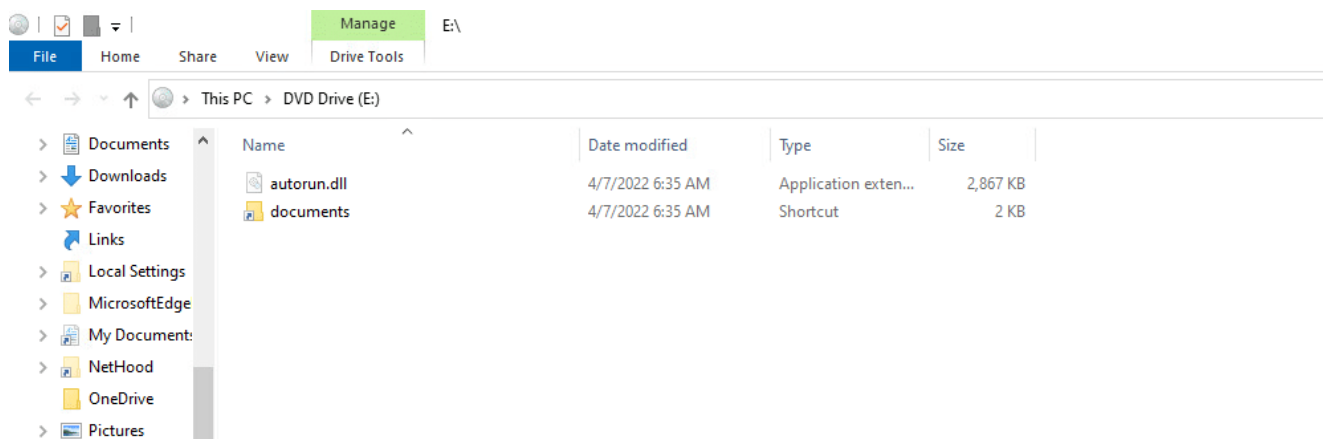
The infection flow

We've handled several incident response (IR) cases where threat actors distributed BumbleBee malware. After the initial infection, the threat actors inject Cobalt Strike shellcode in memory and execute discovery commands to collect info about the victim's network. We believe that threat actors performed this data collection in order to execute the next stage of the infection.

The next stage is probably related to ransomware operations. We're still investigating IR cases in order to find conclusive evidence that the next stage delivers ransomware.

On April 12, 2022, the BumbleBee IAB group was spotted using IMG file format in addition to ISO file format.

You can see an example in the image below.



The IMG file, which contains LNK and DLL

Orion's technical analysis

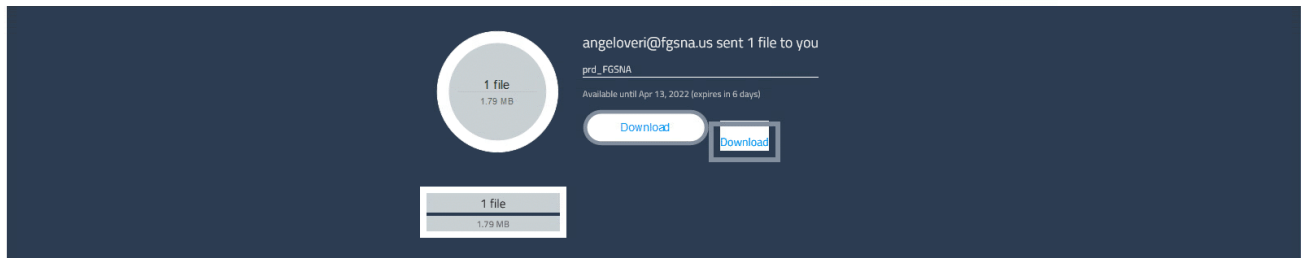
Initial Access

The BumbleBee payload was delivered via a spear phishing email that was sent from a spoofed email address. The email contains a URL link to the legitimate public storage service, TransferXL.

From: angeloveri@fgsna.us via TransferXL <no-reply@transferxl.com>
Sent: Wednesday, April 6, 2022
Subject: [EXTERNAL] angeloveri@fgsna.us sent you 1 file using TransferXL

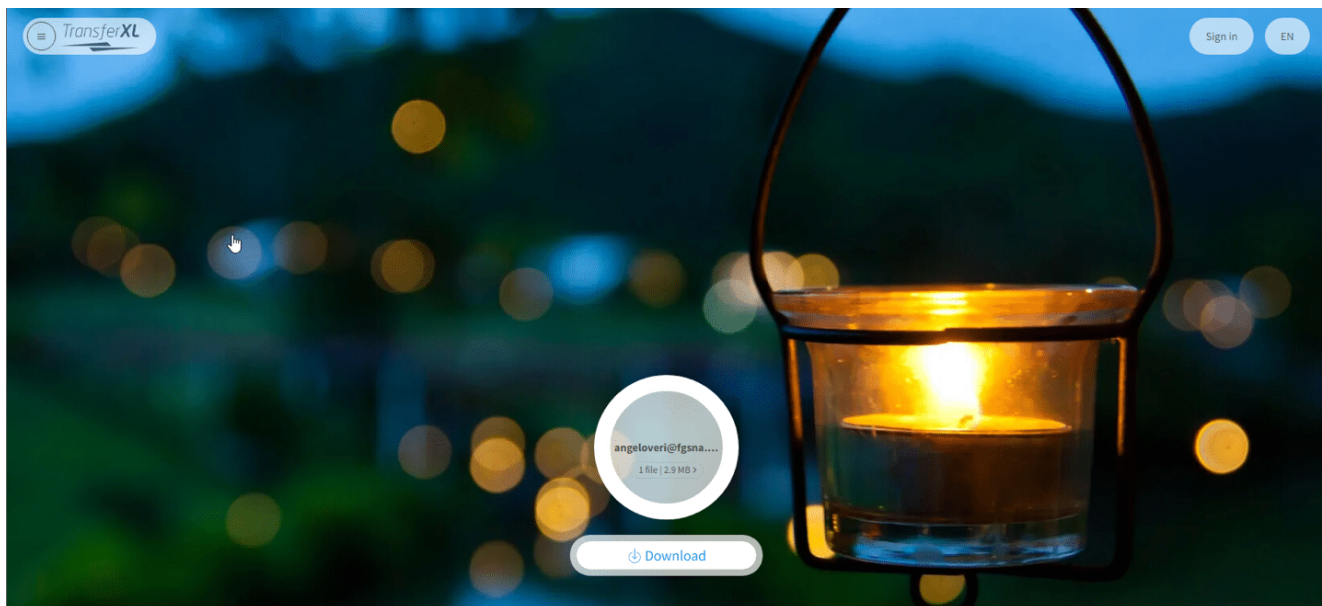
Download now this transfer sent to you by clicking in the link in this email.

If you cannot see this email, [click here](#)



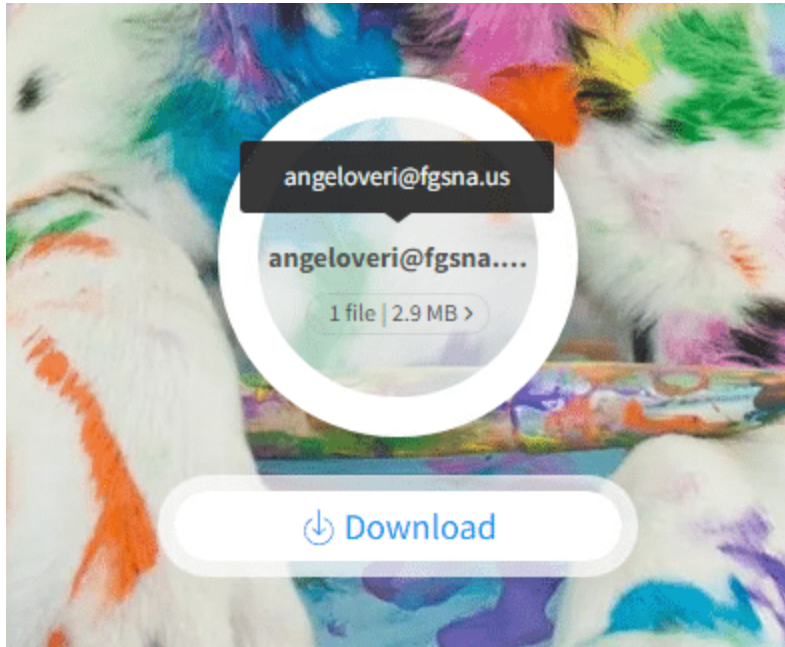
Spear phishing email with a link to TransferXL

Below you'll see the legitimate public storage site, which leads the victim to the link to the malicious file.



TransferXL legitimate public storage services

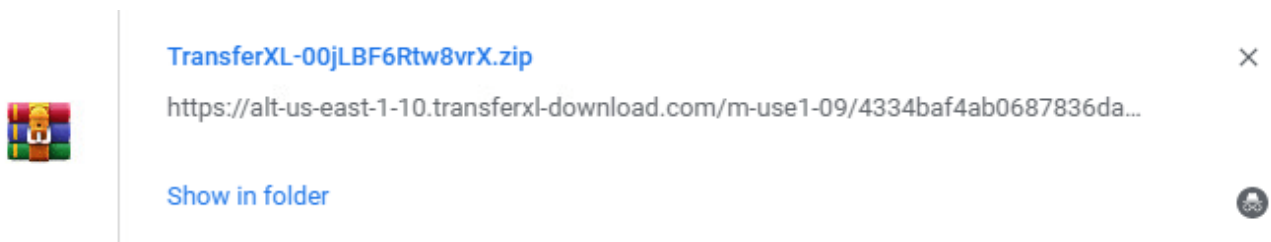
Once they click download, the victim receives a ZIP folder that contains the malicious ISO image files.



Spooferd company email address

Execution

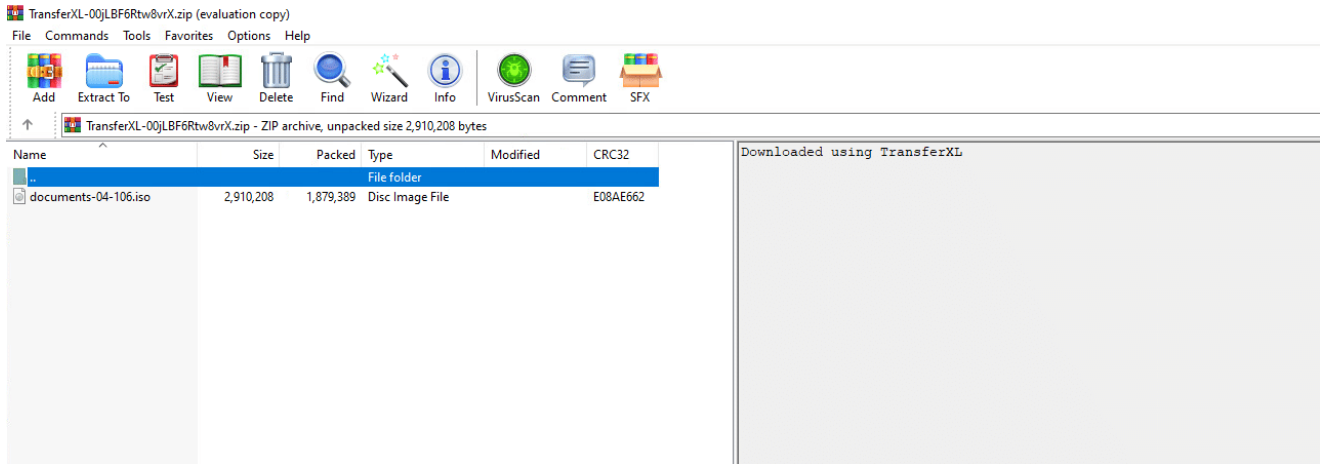
Below is an example of what the ZIP file from the TransferXL link looks like.



ZIP file download from TransferXL

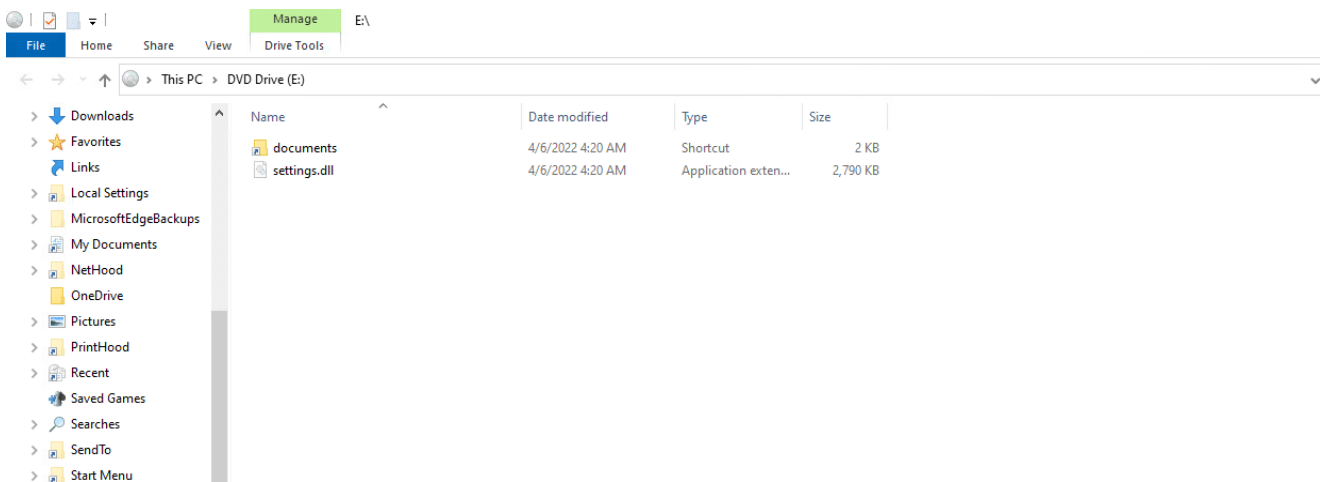
The ZIP file contains an ISO image file with the following name “documents-04-106.iso.” Note that the following ISO image file name pattern was used for all the files that we have analyzed:

documents-[0-9]{1,4}-[0-9]{1,4}\.iso



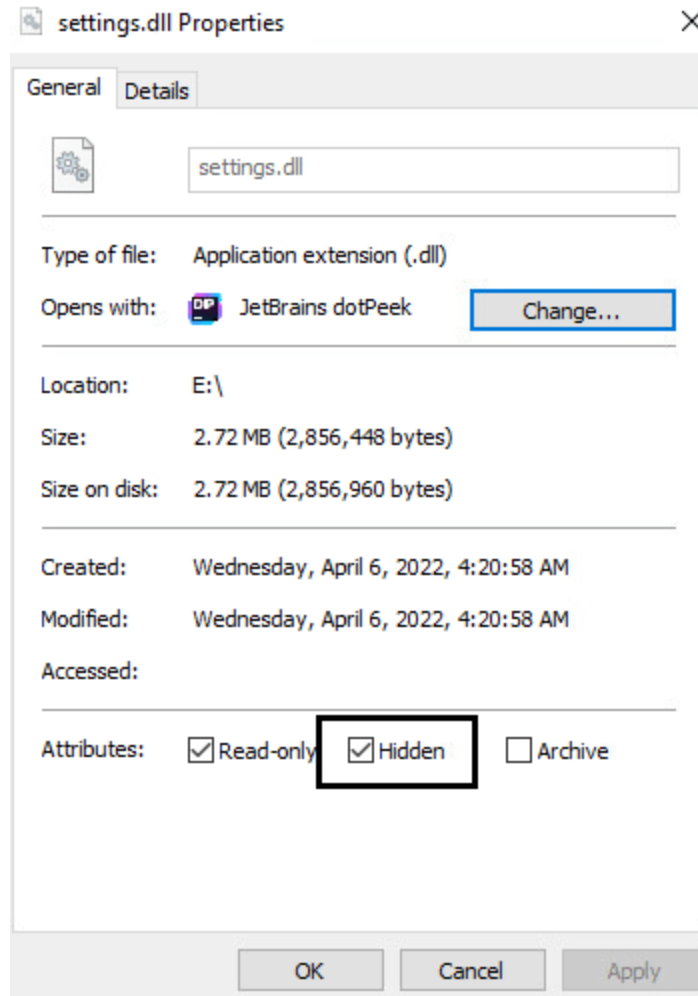
ISO image file

From this step, threat actors rely on the victim (user) interaction with the ISO image file. The threat actors use a masquerading technique by setting the LNK file icon to be a folder icon in order to lure the victim to click on the LNK file:



ISO image file contains LNK and DLL

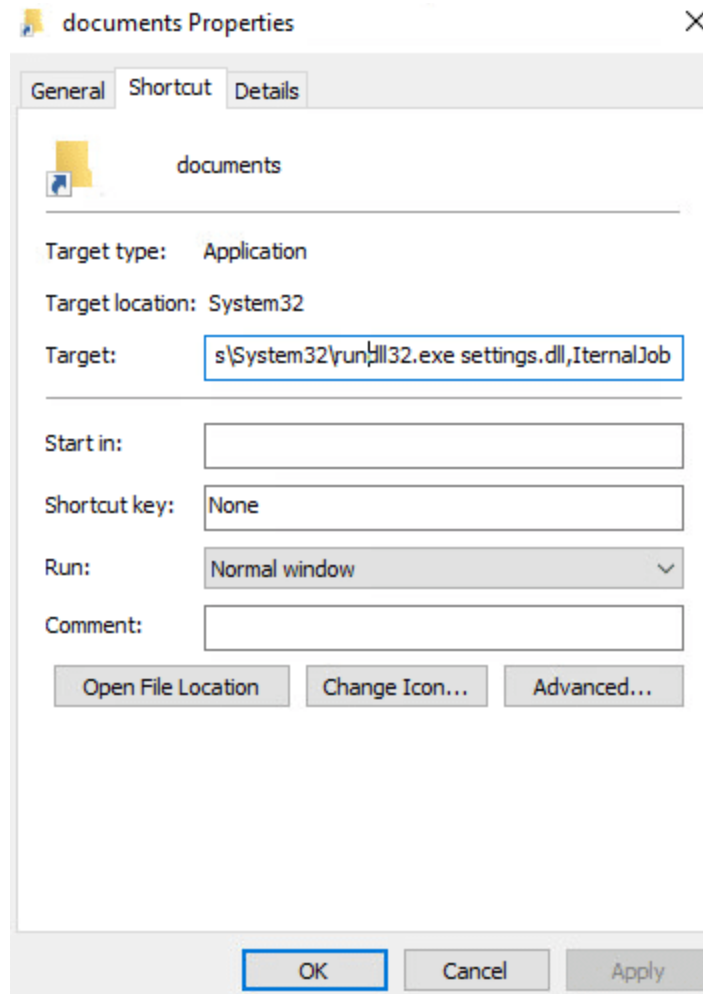
In addition, the DLL payload attribute is set as “Hidden” in order to hide the DLL payload from the user when interacting with the ISO image file:



Hidden attribute for the DLL

The masqueraded LNK file properties show that the execution target is as follows:

C:\Windows\System32\rundll32.exe settings.dll,InternalJob



LNK executes the DLL via rundll32 command

After the initial execution, the BumbleBee DLL is copied to the %programdata%\{RandomDir} directory. In addition to the DLL, a VBS script is also dropped to the same directory:

[a-z]:\programdata\[a-z0-9]{16}\[a-z0-9]{16}\.[vbs|dll]

action	process_path	file_path	new_process_command_line
Write	c:\windows\system32\rundll32.exe	c:\programdata\045241ad770d73bd\8cbc96f0e4e2ae45.vbs	-
Create New	c:\windows\system32\rundll32.exe	c:\programdata\045241ad770d73bd\8cbc96f0e4e2ae45.vbs	-
Execute New Process	c:\windows\system32\wbem\wmiprvse.exe	c:\windows\system32\wscript.exe	wscript.exe C:\ProgramData\045241ad770d73bd\8cbc96f0e4e2ae45.vbs
Execute New Process	c:\windows\explorer.exe	c:\windows\system32\rundll32.exe	'C:\\Windows\\System32\\rundll32.exe' settings.dll,InternalJob
Execute New Process	c:\windows\explorer.exe	c:\windows\system32\rundll32.exe	'C:\\Windows\\System32\\rundll32.exe' settings.dll,InternalJob
Execute New Process	c:\windows\explorer.exe	c:\windows\system32\rundll32.exe	'C:\\Windows\\System32\\rundll32.exe' settings.dll,InternalJob

TTPs indicators during the execution

We have other artifacts from different IR cases, where we have observed the following activity. The screenshot below shows an event that detected a creation of a payload in the %ProgramData%\{Random} directory the DLL payload is a copy of the initial BumbleBee

loader that executed by Rundll32 from the ISO image file:

Time	Parent Process Details.Process Params	Extra Info. Infected File	Extra Info. Infected File MD5	Classification
Mar 1, 2022 @ 18:42:08.000	"C:\Windows\System32\rundll32.exe" disk.dat,ProcessLoad	c:\programdata\{869175ffaf8581a457e78a8bd973c98}.dll	D558E692E638590ED84D728422207EF7	Detection Engine - Malicious Binary - Infected File - File Dumped on the Disk

Copy of the BumbleBee DLL to %Programdata% directory

In other IR cases, we observed an execution flow that's bit different. For example, a LNK that points to the following execution targets:

- cmd.exe /c start rundll32 neqw.dll,InternalJob
- rundll32.exe advpack.dll,RegisterOCX sysctl.exe

Persistence

We detected a scheduled task execution during the BumbleBee infection:

Grandparent process:

svchost.exe -k netsvcs -p -s Schedule

Parent process:

wscript.exe [a-z]:\programdata\[a-z0-9]{16}\[a-z0-9]{16}.vbs

Child process:

rundll32.exe [a-z]:\programdata\[a-z0-9]{16}\[a-z0-9]{16}.dll,{Export}

[S] .rdata:00000001801D0010	0000000A	C	ntdll.dll
[S] .rdata:00000001801D0020	00000005	C	.dll
[S] .rdata:00000001801D0028	00000005	C	.vbs
[S] .rdata:00000001801D0030	0000006C	C	Set objShell = CreateObject("\Wscript.Shell")\r\nobjShell.Run "\rundll32.exe my_application_path, InternalJob"\r\n
[S] .rdata:00000001801D00A0	00000014	C	my_application_path
[S] .rdata:00000001801D00B8	00000018	C (1...	wscript.exe
[S] .rdata:00000001801D00D0	0000000D	C	wscript.exe

Strings from the BumbleBee loader show the VBS script and the execution method

We also observed WMI execution. The VBS file that was executed via a scheduled task, was also executed through WMI:

Grandparent process:
svchost.exe -k DcomLaunch

Parent process:

wmiprvse.exe -Embedding

Child process:

wscript.exe [a-z]:\programdata\[a-z0-9]{16}\[a-z0-9]{16}\.vbs

.rdata:000000001801D70E0	00000016	C (1... ROOT\cimv2
.rdata:000000001801D70F8	00000014	C (1... ole32.dll
.rdata:000000001801D7110	00000012	C CoSetProxyBlanket
.rdata:000000001801D7128	0000000E	C (1... Create
.rdata:000000001801D7138	0000001C	C (1... Win32_Process
.rdata:000000001801D7158	0000002A	C (1... Win32_ProcessStartup
.rdata:000000001801D7184	00000004	C (1...

Strings from the Bumblebee loader show the WMI Win32_Process execution

Defense Evasion

In our labs, we observed that BumbleBee uses several anti-VM methods to avoid detection.

One of the anti-VM checks is related to the VirtualBox product:

```
lea rcx, asc_1801D8CA8 ; "\b"
call sub_180041A90
test eax, eax
mov esi, edi
setz sil
and esi, ebp
call sub_18003E3A0
mov ecx, edi
test eax, eax
setz cl
xor edx, edx ; lpWindowName
and esi, ecx
lea rcx, ClassName ; "VBoxTrayToolWndClass"
call cs:FindWindowW
lea rdx, WindowName ; "VBoxTrayToolWnd"
xor ecx, ecx ; lpClassName
mov rbx, rax
call cs:FindWindowW
test rbx, rbx
jnz short loc_18003D9AA
```

Check for lpWindowName if matches VirtualBox

Other anti-VM artifacts were found after unpacking, as can be seen in the following strings:

Offset	Type	Strings found
001D8573	UNICODE	VBOX_
001D85AB	UNICODE	VBOX_
001D85E3	UNICODE	VBOX_
001D8BE9	UNICODE	VBoxControl.exe
001D868E	UNICODE	VBoxGuest
001D8CDC	UNICODE	VBoxGuest
001DA478	UNICODE	VBoxGuest
001D8891	UNICODE	VBoxGuest.sys
001D8D01	UNICODE	VBoxMiniRdDN
001D8CB4	UNICODE	VBoxMiniRdrDN
001D86DE	UNICODE	VBoxMouse
001DA490	UNICODE	VBoxMouse
001D8851	UNICODE	VBoxMouse.sys
001D878E	UNICODE	VBoxSF
001DA468	UNICODE	VBoxSF
001D88D1	UNICODE	VBoxSF.sys
001D872E	UNICODE	VBoxService
001D8D2C	UNICODE	VBoxTrayIPC
001D8D51	UNICODE	VBoxTrayIPC
001D8DD0	UNICODE	VBoxTrayToolWnd
001D8DA0	UNICODE	VBoxTrayToolWndClass
001D87DE	UNICODE	VBoxVideo
001D8909	UNICODE	VBoxVideo.sys
001D8F58	UNICODE	VBoxVideoW8
001D8F70	UNICODE	VBoxWddm
001D9A68	UNICODE	VMSvc.exe
001D9A80	UNICODE	VMUSvc.exe
001D9A60	ASCII	VMWARE
001D92B8	UNICODE	VMWARE
001D9938	UNICODE	VMWare
001D9868	UNICODE	VMWare\
001D9A58	ASCII	VMware
001D94F9	UNICODE	VMware, Inc.\VMware Tools
001D9948	UNICODE	\\.\HGFS
001D8CD8	UNICODE	\\.\VBoxGuest




















List of strings that are related to VMware and VirtualBox

BumbleBee also detects if it is running within a VM by checking for known services that are related to different VM products:

Offset	Type	Strings recognized as registry key
001D9AF0	UNICODE	SOFTWARE\Microsoft\Virtual Machine\Guest\Parameters
001D9410	UNICODE	SYSTEM\ControlSet001\Control\SystemInformation
001D9E20	UNICODE	SYSTEM\ControlSet001\Services\BALLOON
001D9E70	UNICODE	SYSTEM\ControlSet001\Services\BalloonService
001D8670	UNICODE	SYSTEM\ControlSet001\Services\VBoxGuest
001D86C0	UNICODE	SYSTEM\ControlSet001\Services\VBoxMouse
001D8770	UNICODE	SYSTEM\ControlSet001\Services\VBoxSF
001D8710	UNICODE	SYSTEM\ControlSet001\Services\VBoxService
001D87C0	UNICODE	SYSTEM\ControlSet001\Services\VBoxVideo
001D9D60	UNICODE	SYSTEM\ControlSet001\Services\VirtIO-FS Service
001D9DC0	UNICODE	SYSTEM\ControlSet001\Services\VirtioSerial
001D9ED0	UNICODE	SYSTEM\ControlSet001\Services\netkvm
001D9CC0	UNICODE	SYSTEM\ControlSet001\Services\vioscsi
001D9D10	UNICODE	SYSTEM\ControlSet001\Services\viostor

List of services that are related to VM products

BumbleBee checks whether certain user names reside in the victim's machine by comparing against a hardcoded list of user names. This allows BumbleBee to detect sandboxes and labs that are used for malware analysis:

	.rdata:00000001801D88C8	00000018	C (1... CurrentUser
	.rdata:00000001801D88E0	00000010	C (1... Sandbox
	.rdata:00000001801D88F0	0000000C	C (1... Emily
	.rdata:00000001801D8900	00000010	C (1... HAPUBWS
	.rdata:00000001801D8910	00000012	C (1... Hong Lee
	.rdata:00000001801D8928	00000012	C (1... IT-ADMIN
	.rdata:00000001801D8940	00000010	C (1... Johnson
	.rdata:00000001801D8950	0000000E	C (1... Miller
	.rdata:00000001801D8960	0000000E	C (1... milozs
	.rdata:00000001801D8970	0000001A	C (1... Peter Wilson
	.rdata:00000001801D8990	0000000C	C (1... timmy
	.rdata:00000001801D89A0	00000012	C (1... sand box
	.rdata:00000001801D89B8	00000010	C (1... malware
	.rdata:00000001801D89C8	00000010	C (1... maltest
	.rdata:00000001801D89D8	00000014	C (1... test user
	.rdata:00000001801D89F0	0000000C	C (1... virus
	.rdata:00000001801D8A00	00000012	C (1... John Doe
	.rdata:00000001801D8A20	00000046	C (1... Checking if username matches : %s
	.rdata:00000001801D8A68	0000000E	C (1... VMWare

List of hardcoded usernames which are related to sandboxes and labs

In addition, it uses WMI queries to collect system details and information:

- SELECT * FROM Win32_BaseBoard
- SELECT * FROM Win32_Bus

- SELECT * FROM Win32_ComputerSystem
- SELECT * FROM Win32_Fan
- SELECT * FROM Win32_NTEventlogFile
- SELECT * FROM Win32_OperatingSystem
- SELECT * FROM Win32_PnPDevice
- SELECT * FROM Win32_PnPEntity

Discovery

We found that the threat actors used the AdFind tool to enumerate and map the victim's network. The AdFind tool was found in the %ProgramData% directory.

In the instance we observed, the following commands were used:

- adfind.exe -gcb -sc trustdmp
- adfind.exe -f "(objectcategory=group)"
- adfind.exe -f "(objectcategory=organizationalUnit)"
- adfind.exe -f "(objectcategory=computer)"
- adfind.exe -f "(objectcategory=person)"

Command and Control

After the initial execution, the BumbleBee process (Rundll32) communicated with the Command-and-Control server (C2). We've seen several C2 servers from different IR cases:

- *IP: 23.82.19[.]208:443*
- *IP: 192.236.198[.]63:433*
- *IP: 45.147.229[.]177:433*

property	value
md5	36D49170F3115D378F8B6A3A45B23525
sha1	AE1A95DA9B7488B51C8549C52DE8E2F73C022608
sha256	EED2D5DD3B0FCCD71FA30B79708004E7393E83AAC8566E80808F1162936BC1F2
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z @
file-size	28160 (bytes)
size-without-overlay	n/a
entropy	6.323
imphash	1369F81AACB871DA7C04248B77211BB2
signature	n/a
entry-point	55 8B EC 51 8B 45 0C 89 45 FC 83 7D FC 01 74 02 EB 0D 8B 4D 08 51 8B 55 10 52 E8 C1 FF FF FF B8 01
file-version	n/a
description	n/a
file-type	dynamic-link-library
cpu	32-bit
subsystem	GUI
compiler-stamp	0x624C9623 (Tue Apr 05 12:18:59 2022)
debugger-stamp	0x624C9623 (Tue Apr 05 12:18:59 2022)
resources-stamp	n/a
import-stamp	0x00000000 (empty)
exports-stamp	0x624C9623 (Tue Apr 05 12:18:59 2022)
version-stamp	n/a
certificate-stamp	n/a

PEStudio showing the payload's metadata

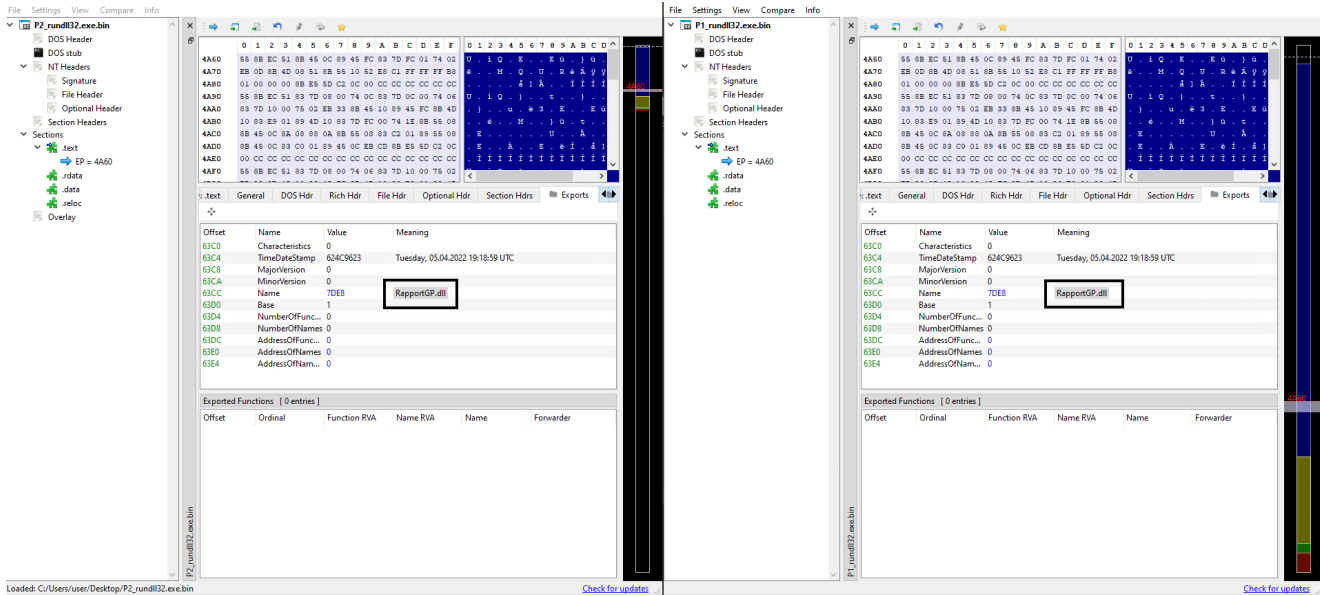
We found a few interesting functions in the payload strings indicating that this payload has process injection capabilities. For example, "CreateProcess," "NtWriteVirtualMemory," "CreateRemoteThread," and "WinExec."

encoding (2)	size (bytes)	location	blacklist (82)	hint (54)	value (382)
ascii	19	0x00005ED8	x	-	NtReadVirtualMemory
ascii	19	0x00005EEC	x	-	NtFreeVirtualMemory
ascii	23	0x00005F00	x	-	NtAllocateVirtualMemory
ascii	14	0x00005F18	x	-	NtResumeThread
ascii	18	0x00005F28	x	-	NtSetContextThread
ascii	23	0x00005F3C	x	-	NtSetInformationProcess
ascii	22	0x00005F54	x	-	NtSetInformationThread
ascii	15	0x00005F6C	x	-	NtSuspendThread
ascii	20	0x00005F7C	x	-	NtUnmapViewOfSection
ascii	11	0x00005FC8	x	-	NtOpenEvent
ascii	20	0x00005FF4	x	-	NtWriteVirtualMemory
ascii	25	0x0000600C	x	-	NtQueryInformationProcess
ascii	23	0x00006028	x	-	NtAdjustPrivilegesToken
ascii	18	0x0000605C	x	-	NtTerminateProcess
ascii	13	0x00006070	x	-	NtOpenProcess
ascii	13	0x00006080	x	-	NtOpenSection
ascii	17	0x000060B4	x	-	RtlExitUserThread
ascii	19	0x000060C8	x	-	KiUserApcDispatcher
ascii	25	0x000060DC	x	-	KiUserExceptionDispatcher
ascii	12	0x000060F8	x	-	NtOpenThread
ascii	19	0x00006108	x	-	RtlDecompressBuffer
ascii	13	0x000061A0	x	-	CreateProcess
ascii	21	0x000061B0	x	-	CreateProcessInternal
ascii	21	0x000061C8	x	-	CreateProcessInternal
ascii	13	0x000061E0	x	-	CreateProcess
ascii	18	0x000061F0	x	-	CreateRemoteThread
ascii	15	0x00006204	x	-	FindFirstFileEx
ascii	15	0x00006218	x	-	FindFirstFileEx
ascii	31	0x00006288	x	-	RtlInstallFunctionTableCallback
ascii	7	0x000062A8	x	-	WinExec
ascii	18	0x00006310	x	-	CreateRemoteThread
ascii	13	0x0000634C	x	-	FindFirstFile
ascii	13	0x0000635C	x	-	FindFirstFile
ascii	16	0x000065AA	x	-	PathFindFileName

PEStudio showing the payload's strings that could be related to process injection

The second payload that we extracted from the .data section is a 64-bit DLL payload:

Both DLL payloads have the same internal name “RapportGP.dll.” An interesting point regarding the payloads internal name is that there is a legitimate DLL named “RapportGP.dll” that is part of a “Trusteer Ltd” product from a computer security division of IBM.

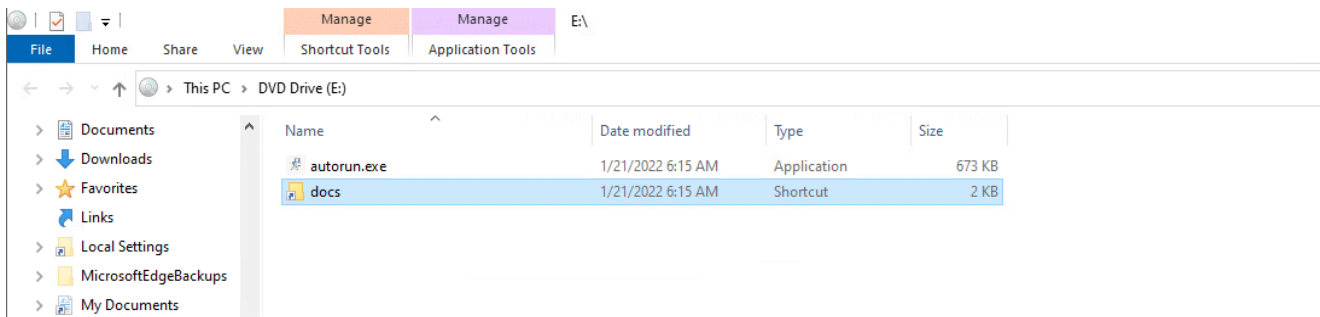


Payloads internal name and TimeDateStamp

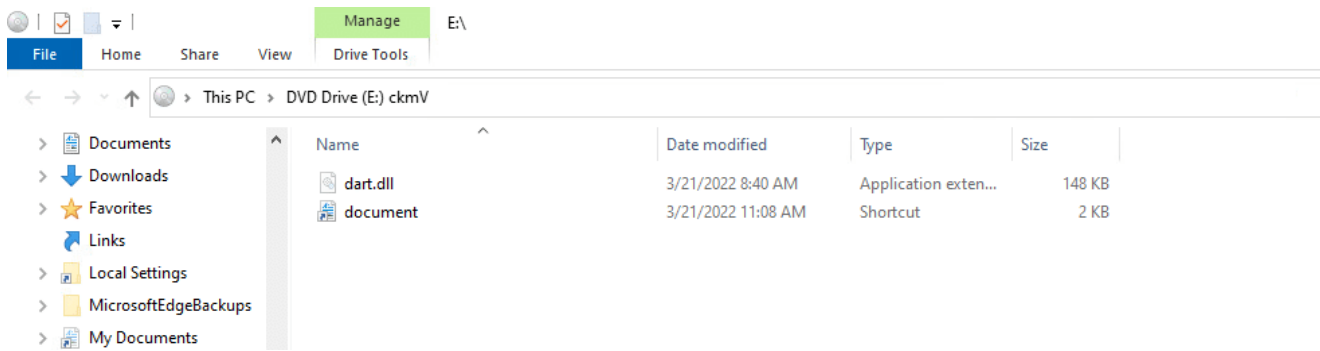
Final notes

BumbleBee threat actors are not the first to change the initial access method from malicious office documents to malicious ISO image files. The ISO image file abuse was also seen a few years ago, but in recent months, we have observed an increase in “ISO campaigns.”

Different threat actors abuse ISO image files to deliver their payloads. For example, BazarISO deploys Bazarloader, and IcedID started to use ISO image files instead of MalDocs like in the two examples below.



Documents-17.iso (Bazarloader)



Invoice_pdf_1.iso (IcedID)

In most of the cases, we've seen that during different IR cases, the campaigns escalated to full-blown ransomware attacks. We believe that IAB groups work and collaborate with ransomware affiliates like CONTI, LockBit, AvosLocker, and more. For example, we observed an IcedID infection that leads to CONTI ransomware attack ([Shelob Moonlight](#)).

The Orion team is constantly monitoring BumbleBee and the IAB group's activities closely and analyzing them to better understand their motivation. As we learn more, we will publish our findings and artifacts to share additional insights for BumbleBee infection to ransomware post-attack chain.

We're expecting to see more malware campaigns that will use the ISO delivery method in the near future. So, stay vigilant.

As a final note, we'd like to share these indicators of compromise with you.

Indicators of compromise:

BumbleBee payload

88F5AE9691E6BCDD4065A420EAF3E3AA32C69605BF564A42FFD8ECD25C9920
4a49e2f06ba48d3a88fdeb83fb8021f3d165535e8ea5319b16a7ebe4da9c0751
08cd6983f183ef65eabd073c01f137a913282504e2502ac34a1be3e599ac386b
186145f84ed6a473ec6bc4afa66bfff156057888938793b12afd17659041ddbba
4063fab9176db3960fa6014173b6c7ba52f19424887f5a6205ff73aa447ada61
53b3ebaa3c485772f8e6abaa0f366ef192137496a7064e015ced4e6fc204b3c8
d74a3f9b35d657516eb53d4e70582f93d22077d3e0936758cc4ef76d5171075d
8f47c3962a7c418bae71fec42bbca9524b72f8f0fd2dd81d1175138f7d20b2f7
c97b8bffcbe424cbc2a6e1135068d071c6f4e8f020fccd2db3dbee3aa80102ac

BumbleBee C2 server

IP: 23.82.19[.]208 Port 443

IP: 192.236.198[.]63 Port 433

IP: 45.147.229[.]177 Port 433

Cobalt Strike C2 server

hojimizeg[.]com - 45.147.228[.]197

notixow[.]com - 23.19.58[.]154

rewujisaf[.]com - 142.234.157[.]176

We hope this was helpful. And remember to check our blog page and follow us on social media to see when we publish updates.

Have questions? [Let us know.](#)